

UNITED STATES DISTRICT COURT  
DISTRICT OF NEW JERSEY

INNOAS INC., a New Jersey corporation,

*Plaintiff,*

vs.

VISTA CAPITAL, LLC, d/b/a  
BANCARDXPRESS; ETHAN PARK, an  
individual; EDUARDO PARK, an  
individual; XYZ CORPS. 1-10  
(fictitious); and JOHN/JANE DOES 1-10  
(fictitious);

*Defendants.*

Civil Action No.: \_\_\_\_\_

**COMPLAINT  
AND JURY DEMAND**

PLAINTIFF INNOAS INC. ("INNOAS" or "Plaintiff") by way of Complaint against the defendants, BANCARDXPRESS; ETHAN PARK, and EDUARDO PARK; and unknown entities or persons to be named; verily avers and SAYS:

**NATURE OF ACTION**

1. This is a case of corporate pirating, computer hacking/unauthorized entry, sabotage/malware insertion, interference with contract/economic advantage, and unfair competition, without limitation, arising from a violation of a non-compete agreement by a former employee in collusion with that employee's subsequent employer.

2. Defendants are in the business of electronically processing credit-card payments. Plaintiff is in business of marketing, installing and maintaining point-of-sale (POS) credit-card processing equipment and software at merchant locations. Defendants expropriated Plaintiff's key data, hacked and damaged Plaintiff's computer capabilities, and unlawfully solicited Plaintiff's customers in furtherance of Defendants' newly launched, competitive service.

## **PARTIES**

3. INNOAS is a for-profit corporation organized and existing under the laws of New Jersey, with a registered office located at 21 Grand Avenue, Suite 111, in the Borough of Palisades Park, County of Bergen. INNOAS is the successor corporation since 2012 to ZionLink Inc. (“ZionLink”); and its former subsidiaries First Payment Solutions, Inc. (“1st Payment”), and The 5th Ave USA, Inc. (“5th Ave”).

4. Upon information and belief, Defendant VISTA CAPITAL, LLC is a corporation organized and existing under the laws of New Jersey, doing business under its trade name BanCardXpress (“BanCardXpress” or “BCX”), having a principal place of business located at 1270 Broadway, Suite 709, in the City of New York; and an office located at 1325 Sterling Boulevard, in the City of Englewood, County of Bergen, within this vicinage.

5. Defendant ETHAN PARK (“Ethan”) is an individual who is listed as one of the general partner of BCX and who represents himself to be the vice president of BCX, with an unknown residential address in the County of Bergen. Ethan Park may be directly liable to Plaintiff for ultra vires conduct.

6. Defendant EDUARDO PARK (“Eduardo”) is an individual with a last-known residential address of 275 Hoym Street, Apt. 5A, in the Borough of Fort Lee, County of Bergen.

7. The defendants XYZ Corporations 1 through 10 are, upon information and belief, businesses, companies, corporations, limited liability companies or partnerships, traditional partnerships, or other juridical or de facto entities, whose identities are unknown to Plaintiff at the current time, but whose may be liable to Plaintiff, under tort law, contract law, or other statutory or common law, pursuant to the laws of New Jersey or the United States.

8. The defendants, John/Jane Does 1 through 10 are, upon information and belief, individuals, professionals or sole proprietorships whose identities are unknown to Plaintiff at the current time, but who may be liable to Plaintiff, under tort law, contract law, or other statutory or common law, pursuant to the laws of New Jersey or the United States.

### **JURISDICTION AND VENUE**

9. This Court has original jurisdiction pursuant 28 U.S.C. § 1331, as claims raised herein are pursuant to the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030.

10. This Court has supplemental jurisdiction over the New Jersey State causes of actions raised herein pursuant to 28 U.S.C. § 1367(a). The State causes of actions raised herein are so related to the claims raised under the CFAA, 18 U.S.C. §1030.

11. Venue is proper under 28 U.S.C. § 1391. Defendant BCX is a corporation organized and existing under the laws of New Jersey and has an office located at 1325 Sterling Boulevard, in the City of Englewood, County of Bergen, State of New Jersey. Defendants Ethan and Eduardo are also residents of New Jersey.

### **FACTS COMMON TO ALL COUNTS**

#### **Credit Card Processing Services**

12. The near-instantaneous clearing of credit-card transactions worldwide is well known today. By way of simplified overview as background, a cardholder must present a valid credit card from an “issuing bank”, using an unexpired account having sufficient credit available. The card is entered into an electronic terminal (i.e., card-reader) at the location of the provider of retail goods or services, generally referred to as the “Merchant”; some terminals may allow entry of a card account number, expiration and security code, allowing credit cards information to be read over the telephone to the merchant instead of physically presenting the card. For small

businesses and retailers, the terminal is typically is connected to a dedicated telephone line provided by the Merchant.

13. After a brief transmission and encoding/encryption delay over a data network, the transaction will be authorized or declined; occasionally, an adjustment may also occur with the transaction (e.g., a gratuity for a meal charged to a credit card after the charge was approved). If the transaction is authorized, the net payment, less the contractual processing fee (typically, 1½% to 2½%), will appear in the Merchant's account with an "acquiring" bank (or the "merchant bank"), generally within a business day or two. A "debit card" option requires the additional entry of a personal identification number ("PIN") code; a refund transaction generally reverses the foregoing process.

14. Accomplishing such convenience in commerce usually engages the services of intermediaries for the 'back-end' processing. While some credit-card providers may provide for direct processing (e.g., American Express), an acquiring or merchant bank generally uses a third-party independent sales organization (ISO) or a membership service provider (MSP) to conduct and monitor the day-to-day activities of their merchant accounts. ISO's and MSP's have relationships with a VISA or MasterCard Association Member institution (i.e., a bank). VISA and MasterCard are not banks but "Card Associations" and clearing houses that set standards and interchange fees for their respective brands, and related activities. Such systems may also provide processing services for other card brands (e.g., Discover, Diners Club) by arrangement.

#### **Relationship and Services of Plaintiff and BanCardXpress**

15. Plaintiff is a leading provider of POS hardware, systems and services, among other 'hi-tech' solutions to a base of Merchants such as restaurants, salons, retail stores, and other commercial or professional establishments that accept credit cards. Plaintiff has been serving and



expanding customer base for about two (2) decades, with an established reputation for responsiveness, high standards for quality and value. Plaintiff serves all Merchants, with a particular focus on the Korean- language community.

16. Plaintiff maintains its computer systems in confidence and with a combination of standard and special security-type procedures and systems, as are updated periodically together with technology, as it evolves and becomes commercially available.

17. The terms ISO and MSP are often used synonymously, although MasterCard tends to prefer MSP. Therefore, it is common for such third-party businesses to refer to themselves as “an ISO/MSP for” a given institution.

18. Defendant BCX website describes itself as “a registered ISO/MSP of Elavon[, Inc.,] a wholly owned subsidiary of U.S. Bancorp, Minneapolis, MN” and also as “a registered ISO/MSP of Wells Fargo Bank, N.A., Walnut Creek, CA”.

19. Upon information and belief, Defendant BCX has expanded its field of business and/or service to that which plaintiff is engaged in or provides, and has therefore become Plaintiff’s direct competitor.

20. Both Plaintiff and BCX serve the same Merchants. Plaintiff’s direct contractual relationship with BCX commenced with ZionLink, and memorialized in a certain Referral Agreement, as amended, and an Independent Agent Service Agreement (collectively the “Innoas/BCX Agreements”).

21. To accept credit-cards as part of its business, a Merchant must sign a “BanCardXpress Merchant Service Agreement” (“BCX-Merchant Agreement”) with BCX as the Merchant’s exclusive provider of card-processing services. Plaintiff is BCX’s authorized

representative to provide and maintain the credit-card terminal. Section 3.3 of the BCX-Merchant Agreement provide that the

Merchant shall maintain an adequate inventory of supplies in the premises, which may be provided by the Company. Merchant shall, in good faith, cooperate in providing maintenance services on the credit card machine. Merchant shall in no other instances permit anyone other than an authorized representative or designee of Company to perform any service or repair work on the credit card machine without Company's prior written consent. Merchant shall be responsible for the costs of maintenance, servicing and/or repairs of the credit card machine, including parts and labor, . . . . Merchant shall in no other instances permit anyone other than an authorized representative or designee of Company to perform any service or repair work on the credit card machine without Company's prior written consent. Merchant shall be responsible for the costs of maintenance, servicing and/or repairs of the credit card machine, including parts and labor[.]

22. Plaintiff has independent contracts with the Merchants it serves. To obtain hardware, software and service from INNOAS, each Merchant must sign an INNOAS Sales and Service Agreement (the "Plaintiff-Merchant Agreement"), for an initial term of three (3) to five (5) years, depending upon the configuration ordered, automatically renewable for successive two (2) year terms. Plaintiff-Merchant Agreement §§ 7.4, 7.5. After a 90-day trial period, § 6.2, Plaintiff becomes the sole provider of on-site services to the Merchant:

Company shall serve as the EXCLUSIVE merchant services provider for the User's premises. The merchant shall not allow the placement or services of any other credit card machine from another provider nor subscribe to any other third party processor during the duration of this Agreement. [Id. § 7.1. (emphasis in original)]

23. As a consequence of a Merchant having executed a BCX-Merchant Agreement and Plaintiff-Merchant Agreement with Plaintiff as BCX's agent, a Merchant is bound during the term of these contracts to do its card-processing business exclusively with Plaintiff and BanCardXpress.

#### **Relationship of Plaintiff and Eduardo Park**

24. Defendant Eduardo is a former employee of Plaintiff. His employment with Plaintiff's predecessor ZionLink commenced in 2009. When Eduardo was hired, he lacked skills

in computer technology. Plaintiff invested significant time and money in his training and guidance, to the point where Eduardo became the employee in charge of computer hardware and software setup, as well as management. Over his seven (7) year employment, Eduardo became a confidant of the CEO of Plaintiff.

25. Eduardo served as a general manager for both Plaintiff and ZionLink. Eduardo's management duties for Plaintiff dealt with all contracts with customers, managing customers, including the creation of accounts, connectivity and collaboration remotely using electronic mail and LogMeIn, Inc. software. LogMeIn products facilitate access by system administrators and are used to remotely located computers.

26. In addition, Eduardo dealt with technology dealers, partners, resellers, and vendors. Eduardo had responsibility for human resources, including the authority to hire and fire employees. The foregoing list is not exhaustive; Eduardo had 'dotted-line' responsibility for a number of functions when needed.

27. In early 2010, Plaintiff's predecessor took steps to formalize and better protect its confidential information. On or about April 1, 2010, Eduardo executed a confidential, integrated Employment Agreement dated April 1, 2010 (the "Employment Agreement") in favor of "ZionLink, Inc (in association with First Payment Solutions, The 5th Ave and any future associated businesses)" for the position of "Computer hardware, Software Setup, Management". Employment Agreement, preamble, § 4.1. Eduardo is the defined "Employee"; Plaintiff INNOAS is the successor, or "future associated business[,] described in the Employment Agreement and defined therein as the "Company". The Employment Agreement automatically renews annually. Employment Agreement § 2.1.



28. The integrated Employment Agreement provides for the protection of Plaintiff's confidential and trade secret information. Confidential information is defined in § 6.4 as:

[§] 6.4.1.1.

Business, management, production, marketing, sales techniques and arrangements, financial information, customer information (current, past and prospective), and/or information relating to the Company and its employees that, if released to an outsider, will have a negative effect on the Company.

[§] 6.4.1.2.

All Company produced/manufactured item(s), good(s) and service(s) shall be deemed extremely confidential these include and are not limited to: source and object codes, flow charts, algorithms, coding sheets, routines, sub-routines, compilers, assemblers, design concepts and related documentation and manuals.

[§] 6.4.1.3.

All other material or information related to the business or activities of the Company which are not generally known to the others engaged in similar businesses or activities.

Employment Agreement § 6.5 prohibits Eduardo from direct competition with Plaintiff within Plaintiff's fields and industry for a reasonable minimum period of six (6) months following termination.

29. Due to the remote, worldwide nature of the technology, the Employment Agreement defines no restricted geographical area or radius, as technology and a Korean-speaking clientele render no meaningful limitation practicable.

**Defendant Eduardo Park's Substantial Access to Plaintiff's Sensitive Business Data**

30. Eduardo's broad managerial responsibility came with access to Plaintiff's confidential information and trade secrets. There are essentially no INNOAS data to which Eduardo did not have the authority to view and manage. This included codes and passwords to security and protection measures, including those for LogMeIn.

31. Accordingly, the Employment Agreement required Eduardo to keep Plaintiff's confidential and trade secret information indefinitely. More particularly, it provides that



[e]xcept as may be required in the performance of the duties described hereunder, Employee shall not, during the term of this Agreement, or at any time after the termination thereof, disclose to any person, corporation, business or other legal entity, for any purpose whatsoever, any business, financial, technical or other information of the Company that is confidential in nature, or not generally or publicly known, including, but not limited to, its products, prices, terms of sale, customers, suppliers, practices, employees, affiliates, and future intentions/goals. Upon breach of these terms, the Employee hereby agrees to be held responsible for any and all damages and will be held accountable for any and all compensations and reparations directly associated with said breach.

Id. § 6.1 (emphasis added).

32. Plaintiff reasonably relied on Eduardo's assurances, technical skills in which Plaintiff had invested in Eduardo, and adherence to the terms of the Employment Agreement to which Eduardo bound himself.

#### **Defendant Eduardo Park's Separation from Plaintiff**

33. After more than seven (7) years of service, Eduardo resigned from Plaintiff, effective January 25, 2016. It appeared Eduardo separated from Plaintiff's employment on amicable terms, for another opportunity. Plaintiff reminded Eduardo of his surviving obligations under the Employment Agreement, although he had failed to give Plaintiff the requisite two (2) months' notice under § 2.2 of the Employment Agreement.

34. One surviving obligation on Eduardo's separation is set forth in § 6.5 of the Employment Agreement: "Upon termination . . . [Eduardo Park] hereby agree[s] to refrain from engaging in any activities associated with the fields and industries in which the Company is engage[d] for a minimum duration of 6 months." Notwithstanding this restriction, Eduardo accepted immediate employment with Defendant BCX.

35. Eduardo had ample opportunity to copy and remove critical data from Plaintiff's systems before his departure.

### **Unauthorized Access, Hacking, Copying, and Sabotaging of Plaintiff's Critical Systems**

36. In less than two (2) months later Eduardo's separation with Plaintiff, by March 2016, Plaintiff's computer systems installed at Merchant sites were being accessed, including with faked source addresses and virtual private networks (VPN), but not discovered by Plaintiff despite diligence until December 2016. LogMeIn event logs showed frequent access attempts and irregularities from VPN access from December 8th through the 21st. Plaintiff had spent most of the year attempting to identify and solve the anomalies using industry-standard tools and techniques. Changing passwords caused access failures but proved insufficient.

37. Investigating and trying to ascertain and eliminate threats to Plaintiff's core services were a major distraction and financial drain, negatively affecting its customer service and support.

38. With the assistance of MasterCard, in 2017, Plaintiff sought the services of a forensic specialist, technically a qualified security assessor (QSA). By May, Plaintiff had engaged a nonparty QSA, Foregenix Ltd. ("Foregenix"), to investigate Plaintiff's POS systems. Foregenix is based in a suburb of London with an office in Boston. A Bloomberg business overview describes Foregenix as "provid[ing] forensic investigations, cardholder data discovery, information security, and compliance services for the payment card industry (PCI)." PCI forensic investigations are referred to as "PFI".

39. Commencing the end of May 2017, Foregenix investigated for several months. In September 2017, Foregenix issued a detailed 65-page PFI Report for Plaintiff. The PFI Report is confidential and complex. Foregenix confirmed multiple intrusions into Plaintiff's systems back to late 2016, primarily through compromised LogMeIn software, and hacking through remote servers, including servers in Arizona and the Netherlands.

40. The intruder had sufficient information and sophistication to install and activate destructive malware, and to overcome the efforts of security software, including Microsoft Security Essentials, to quarantine it.

41. Plaintiff's sensitive, confidential data were completely extracted. The intentional nature of the surreptitious extractions were confirmed by Foregenix' detection of traces of "clean-up" software used to hide the intruders' virtual tracks. Some digital evidence was inadvertently lost by Plaintiff's "re-imaging" efforts to cleanse its systems of malicious code.

### **Criminal Investigation**

42. Based upon Foregenix' findings, Plaintiff duly reported the intrusions, theft of critical data, and economic losses to the Palisades Park Police Department, which referred the case to the Bergen County Prosecutor's Office.

### **Eduardo's/BanCardXpress' Anticompetitive Merchant Solicitation and Imposition of Fees**

43. Plaintiff suspected Eduardo and his new employer BCX of the intrusions given the extent, and Eduardo's expansive knowledge of Plaintiff's systems and security. Damage to Plaintiff's goodwill and revenues were increasing.

44. In an effort to isolate the source of intrusions, as well as to mitigate its losses, in or around December 2016, Plaintiff began to open, refer, and transition selected Merchant accounts to a different ISO/MSP and track whether any hacking occurred.

45. In retaliation, BCX back-charged \$1,000 in fees to at least two (2) of Plaintiff's customers through the ACH (automated clearing house) network. Each ACH transaction requires express authorization, but BCX hit these Merchants' accounts without such notice.



46. Plaintiff strongly protested these “fees” for porting Plaintiff’s Merchant/customers to other ISO/MSP servicers. Eduardo promised Plaintiff that BCX would reverse those ACH transactions and refund the money to Plaintiff’s customers, but failed to do so.

47. In the meantime, BCX developed its own sales and service group to compete with Plaintiff’s, while Plaintiff continues to service other BCX Merchants. BCX and Eduardo have been soliciting Plaintiff’s Merchant-customers using Plaintiff’s confidential and trade secret information in violation of the Employment Agreement.

48. It is evident that defendant Eduardo, as agent under the direction of the principal of BCX, used Plaintiff’s data in breach of his Employment Agreement, and duties of loyalty, good faith and fair dealing to Plaintiff, and to curry favor with his new employer and codefendant, BCX, by improperly enhancing BCX’s ability to compete with Plaintiff and/or to undercut Plaintiff’s prices using the information misappropriated from Plaintiff.

49. In furtherance of BCX’s unfair and anticompetitive practices, and retaliation, in mid-August 2017 its officer, Defendant Ethan, sent Plaintiff’s customers a written “Merchant Advisory Notice” under BCX’s letterhead, purporting to advise Merchants that it “ha[d] terminated its business relationship with Innoas”, but which strongly implied that Plaintiff had broken the law, and that Merchants’ data were somehow compromised by Plaintiff, cautioning that:

it is very important for all merchants to maintain the integrity of its [sic] card transactions in order avoid [sic] fraudulent transactions. BanCardXpress makes sure that its merchants are in compliance with all applicable laws and regulations promulgated by the Payment Networks and security guidelines and requirements established by the Card Associations.

BCX’s letter went on to threaten Plaintiff’s clientèle with “a breach of contract, subject to legal action, including but not limited to reimbursement for all litigation costs and attorney fees” should any Merchant “change its processing company prior to the end of the contractual term”.

50. At about the same time, Ethan and/or BanCardXpress also wrongfully attempted to terminate the Innoas/BCX Agreements, and threaten Plaintiff, falsely asserting that Plaintiff

compromised the integrity of the card transactions processed with the [] Merchants and failed to comply with all applicable laws and regulations promulgated by the Payment Networks and security guidelines and requirements established by the Card Associations. . . . BanCardXpress will withhold all payments to [Plaintiff] for noncompliance with the terms of the Agreements and material breach of the Agreements.

Moreover, BCX threatened “legal action, including but not limited to reimbursement for all litigation costs and attorney fees” to BCX if Plaintiff were to assist its clients transfer to another ISO/MSP.

51. The intended effect of Defendants’ combination of impairing or infecting Plaintiff’s computer systems and stealing data, the need to dedicate substantial resources to investigate, repair and recover these systems and data; and Defendants’ solicitation of Plaintiff’s customers using Plaintiff’s own confidential and trade secret information stolen by malware and/or by Eduardo in violation of his Employment Agreement, threatening Plaintiff and Plaintiff’s customers, and keeping these customers captive, was and is to have a devastating impact on Plaintiff’s business, reputation and revenues, and ultimately put Plaintiff out of business, taking Plaintiff’s business for BCX.

52. Plaintiff’s damages are ongoing and, to the extent possible, being quantified.

53. Plaintiff will suffer irreparable harm to their business, reputation and goodwill as a direct and proximate result of Defendants’ misconduct if Defendants are not enjoined therefrom.

**COUNT ONE – PERMANENT INJUNCTION – PROHIBITORY AND MANDATORY  
(as against all Defendants)**

1. Plaintiff repeats the allegations set forth in the preceding paragraphs as if fully set forth herein verbatim.

2. As set forth above, Defendants are in possession of sensitive and proprietary information concerning products and software responsible for transactions worth many millions of dollars.

3. Plaintiff would be irreparably harmed if Defendants were not enjoined from having, disseminating or using Plaintiff's data in any way, including without limitation, reputational injury and loss of goodwill.

4. Moreover, the pecuniary and business interests of Plaintiff's Merchants and their cardholders may be jeopardized by Defendants' activities.

5. Defendant Eduardo was under preexisting common law, contractual and statutory duties to ensure the privacy, safety and security of Plaintiff's data and systems.

6. Plaintiff's raise meritorious issues under established law.

7. The balance of the equities significantly favors Plaintiff.

8. The public interest significantly favors Plaintiff.

9. During the pendency of this litigation all Defendants should be prohibited, restrained and enjoined from accessing, copying, deleting, possessing, transferring or in any way using Plaintiff's data; further, Defendants should be compelled to surrender Plaintiff's data and submit their computes, digital equipment, data and logs for forensic analysis.

**COUNT TWO – COMPUTER FRAUD AND ABUSE ACT (CFAA), 18 U.S.C. § 1030  
(as against all Defendants)**

1. Plaintiff repeats the allegations set forth in the preceding paragraphs as if fully set forth herein verbatim.

2. Plaintiff's computers, upon which its confidential, proprietary and trade secret information are stored, are used in and/or affect interstate or foreign commerce or communication.



As such, Plaintiff's computers are protected computers within the meaning of the federal Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(e)(2)(B).

3. Defendants knowingly accessed one or more protected computers without authorization or exceeding the access authorized, and thereby obtained information from one or more protected computers, in violation of CFAA, § 1030(a)(2)(C).

4. Defendants knowingly, and with the intent to defraud, and by means of such conduct furthered the intended fraud and obtained confidential, proprietary and trade secret information which are of value to Plaintiff, in violation of § 1030(a)(4).

5. Defendants' access, copying, retention and use of such data from protected computers affecting the cardholder accounts of the public, comprises a threat to public safety, in violation of § 1030(c)(4)(A)(i)(IV)–(VI).

6. Eduardo conspired with BCX and other Defendants to be discovered in furtherance of access to, and theft of, information from protected computers in violation of CFAA, § 1030.

7. Plaintiff has suffered damage or loss by reason of a violation or violations of § 1030, and discovered its loss within the immediately preceding two (2) years. As such, Plaintiff may maintain a civil action against Defendants for compensatory damages and injunctive relief or other equitable relief, pursuant to CFAA, § 1030(g).

**COUNT THREE – RACKETEERING ACTIVITY, N.J.S.A. § 2C:41-1 *et seq.* (RICO)  
& COMPUTER RELATED THEFT, N.J.S.A. § 2C:20-23  
(as against all Defendants)**

1. Plaintiff repeats the allegations set forth in the preceding paragraphs as if fully set forth herein verbatim.

2. Defendant Eduardo was an insider who enjoyed password or code-based access to information.

3. BCX hired Eduardo at or about the time the unauthorized accessing and copying of data commenced. Eduardo is in a close association with BCX, and is an agent thereof or otherwise authorized to act on behalf of Elavon, Inc./U.S. Bancorp, and Wells Fargo Bank, N.A.

4. Eduardo, in violation of Plaintiff's established internal policies, and in concert with the other Defendant(s), did purposefully or knowingly, and without authorization or in excess of authorization, access Plaintiff's data, database(s), computer storage media, computer program(s) and software including without limitation Plaintiff's key data, software, computer, computer system(s) and network.

5. Eduardo and/or BCX, or an unknown entity on his/its/their behalf, copied Plaintiff's data on multiple occasions, without prior authorization or permission, express or implied.

6. Defendants took and transferred Plaintiff's confidential information for the benefit of BCX and used Plaintiff's electronic mail and LogMeIn software and systems.

7. Eduardo also took and transferred such information to BCX which, together with Eduardo, are in possession of Plaintiff's sensitive, confidential and proprietary information.

8. Eduardo, BanCardXpress, XYZ Corps. 1-10 and John/Jane Does 1-10, although not a legal entity form an enterprise.

9. Defendants are knowingly and purposefully using said information, and directly and proximately causing severe damage and injury to Plaintiff.

10. Such theft constitutes racketeering activity in violation of New Jersey's Racketeer Influenced and Corrupt Organizations Act.

**COUNT FOUR –NEW JERSEY COMPUTER RELATED OFFENSES ACT  
N.J. Stat. Ann. § 2A:38A-1 to -6 (as against all Defendants)**

1. Plaintiff repeats the allegations set forth in the preceding paragraphs as if fully set forth herein verbatim.

2. Plaintiff is an “enterprise” within the meaning of the New Jersey Computer Related Offenses Act (CROA), N.J.S.A. § 2A:38A-3.

3. Each of BCX, Eduardo, Ethan and a colluding entity is an “actor” within the meaning of CROA, § 2A:38A-3.

4. Defendants purposefully, knowingly and without authorization took data or a database, computer program(s), or software existing internally or externally to Plaintiff’s computer, computer system or computer network, in violation of CROA § 2A:38A-3(a).

5. Defendants purposefully, knowingly and without authorization accessed or attempted to access Plaintiff’s computer, computer system or computer network, in violation of CROA § 2A:38A-3(c).

6. Defendants purposefully and knowingly accessed, and recklessly obtained data or a database, computer program(s), or software existing internally or externally to Plaintiff’s computer, computer system or computer network, in violation of CROA § 2A:38A-3(e).

7. Defendants purposefully, knowingly accessed and recklessly inserted malicious software into Plaintiff’s data or a database, computer program(s), or software existing internally or externally to Plaintiff’s computer, computer system or computer network, in violation of CROA § 2A:38A-3(e).

8. Eduardo’s violations of CROA have caused monetary harm to Plaintiff, in an amount to be determined by the trier of fact, pursuant to CROA § 2A:38A-4.



9. Plaintiff comprises an enterprise suffering injury, loss or damage and, absent injunctive relief, will continue to suffer nonmonetary, immediate and irreparable harm. Plaintiff is therefore entitled to relief enjoining actions causing damage or any acts in furtherance thereof, pursuant to CROA § 2A:38A-5.

**COUNT FIVE – NEW JERSEY TRADE SECRETS ACT  
N.J. Stat. Ann. § 56:15-1 to -9 (as against all Defendants)**

1. Plaintiff repeats the allegations set forth in the preceding paragraphs as if fully set forth herein verbatim.

2. BCX, Eduardo, Ethan and the defendants to be discovered knew, or had reason to know that Plaintiff's confidential computer information comprised trade secrets within the meaning of the New Jersey Trade Secrets Act (NJTSA), N.J.S.A. § 56:15-1 to -9.

3. Plaintiff's trade secret information derived independent economic value from not being generally known, including without limitation Plaintiff's computer stored data about proprietary goods and relationships, service needs, Merchant experience, pricing strategy and markets, information that is not generally known or readily obtained or derived.

4. Plaintiff had not given actual or implied consent to disclose its confidential or trade secret information. In fact, Plaintiff required employees with access to trade secret information, especially Eduardo, to be bound by an employment contract to prevent disclosure.

5. Eduardo used improper means to acquire Plaintiff's trade secret information in violation of NJTSA, § 56:15-2.

6. Eduardo disclosed Plaintiff's trade secret information to BCX, and other Defendant to be discovered prior to a material change of position in violation of NJTSA § 56:15-2.

7. Defendants Eduardo, BCX, Ethan, and the Defendants to be discovered knew, or had reason to know, that the trade secret information was acquired by improper means in violation of NJTSA § 56:15-2.

8. All Defendants intended to use this information for purposes of unfair competition against Plaintiff.

9. As a direct and proximate result of Defendants' wrongful disclosure of Plaintiff's trade secret information, Plaintiff has suffered damages.

**COUNT SIX – COMMON LAW MISAPPROPRIATION OF TRADE SECRET  
& CONFIDENTIAL INFORMATION (as against all Defendants)**

1. Plaintiff repeats the allegations set forth in the preceding paragraphs as if fully set forth herein verbatim.

2. Plaintiff's digitally stored information comprised trade secrets.

3. Plaintiff derives independent economic value from the fact that its computer information comprises data about proprietary goods and relationships, pricing strategy and markets, information that is not generally known or readily obtained or derived.

4. Plaintiff took precautions to maintain the secrecy of its computer data including without limitation, requiring employees to execute an Employment Agreement. Defendant Eduardo executed such an Employment Agreement.

5. Plaintiff communicated information about its computer data, sensitive, proprietary and trade secret information to Defendant Eduardo in confidence.

6. Eduardo disclosed and used those data in breach of said confidence.

7. BCX is a competitor of Plaintiff. BCX acquired Plaintiff's trade secret information with knowledge of Eduardo's breach of confidence.

8. Defendants BCX, Ethan, and Eduardo, together with persons and entities to be discovered, are using and attempting to use Plaintiff's trade secret information to Plaintiff's detriment.

**COUNT SEVEN – UNFAIR COMPETITION  
(as against all Defendants)**

1. Plaintiff repeats the allegations set forth in the preceding paragraphs as if fully set forth herein verbatim.

2. The misappropriation and use of Plaintiff's confidential information by Defendants BCX, Eduardo, Ethan and the other Defendants to be discovered violate fair play.

3. Defendants' misappropriation and use of Plaintiff's confidential information constitute common law unfair competition.

4. Defendants' unlawful access, sabotage and deletion of Plaintiff's software systems, confidential and trade secret information constitute common law unfair competition.

5. As a direct and proximate result of Defendants' unfair competition, Plaintiff has been damaged.

**COUNT EIGHT –COMMON LAW FRAUD  
(as against all Defendants)**

1. Plaintiff repeats the allegations set forth in the preceding paragraphs as if fully set forth herein verbatim.

2. Beginning in 2009 and through 2016, Eduardo assured Plaintiff of his commitment to his professional obligation and necessity to Plaintiff's business to maintain the confidentiality and integrity of its computer systems.



3. Eduardo represented that he had Plaintiff's interests at heart. Eduardo made these representations to gain access to Plaintiff's computer passwords, codes, sensitive and trade secret information.

4. BCX and/or Ethan hired Eduardo knowing he had Plaintiff's confidential and trade secret information. BCX supported Eduardo's plans and activities to damage Plaintiff's business.

5. BCX, Ethan, and Eduardo surreptitiously extracted Plaintiff's confidential information via remote servers with collaborative software and/or malicious code before erasing traces of his activities.

6. There was no legitimate purpose for Defendants' access, copying and deleting of Plaintiff's data. Defendants knew, or reasonably should have known, Plaintiff would not have consented to such intrusions.

7. Notwithstanding Defendants' representations, BCX, Ethan, Eduardo, and Defendants to be discovered knowingly accessed, copied, sabotaged, and deleted or purged Plaintiff's confidential and trade secret information.

8. After becoming BCX's agent/employee, Eduardo acted in the role of an ordinary businessperson or manager, representing to Plaintiff that Defendants were trading with Plaintiff in support of their mutual Merchant customers' best interests, for reasons including to lull Plaintiff into continuing to trade with BCX.

9. Defendant's representations were material representations.

10. At the time of the representations, Defendants knew the representations to be false. In fact, Eduardo as an agent of BCX, was in the process of preparing to attack Plaintiff's systems for the purpose of accessing and receiving Plaintiff's confidential and trade secret data, installing malicious software, and deleting traces of Defendants' unlawful activities.

11. Such representations were made with the intent that Plaintiff would rely upon them.
12. Plaintiff reasonably relied upon Defendants' representations.
13. As a proximate result Plaintiff suffered damages.
14. The conduct of Defendants was intentional, willful, wanton, and malicious.
15. Defendants' actions constituted both legal and equitable fraud.
16. Plaintiff is entitled to punitive damages and the reasonable expenses of litigation.

**COUNT NINE –TORTIOUS INTERFERENCE WITH BUSINESS RELATIONSHIPS/  
PROSPECTIVE ECONOMIC ADVANTAGE (as against all Defendants)**

1. Plaintiff repeats the allegations set forth in the preceding paragraphs as if fully set forth herein verbatim.

2. Plaintiff has contractual relationships with customers and Merchants who use Plaintiff's equipment and services. Some of these relationships are existing and Plaintiff is pursuing other business opportunities using their confidential business information.

3. Plaintiff had a reasonable expectation of economic advantage.

4. Eduardo, as Plaintiff's former employee, had knowledge of Plaintiff's contractual relationships.

5. BCX and Ethan, as both a contracting party and competitor of Plaintiff, had actual knowledge of the contractual relationships between Plaintiff and Plaintiff's customers as well as of the confidentiality and significance of Plaintiff's data.

6. Defendants interfered with Plaintiff's contractual relationships in order to divert revenue from Plaintiff; undercut Plaintiff's business with Plaintiff's customers; inflate Plaintiff's cost of doing business, including without limitation by dedicating significant resources to the detection, investigation and correction of Defendants' unlawful copying and destruction of Plaintiff's data; damage Plaintiff's good name and reputation; and ultimately put Plaintiff out of

business or replace Plaintiff with BCX or related entity as the Merchants' sole supplier of Plaintiff's equipment and services.

7. Defendants induced or otherwise sought to cause Merchants to breach their various contractual duties with Plaintiff. This conduct was intentional.

8. Defendants' conduct was without justification or excuse.

9. Defendants have so acted intentionally and with malice, and have engaged in such conduct that is wrongful and without justification or excuse.

10. As a proximate result, Plaintiff has been damaged.

**COUNT TEN – TORTIOUS INTERFERENCE WITH CONTRACT  
(Against All Defendants)**

1. Plaintiff repeats and realleges the allegations of all preceding paragraphs as though fully set forth at length herein.

2. Defendants are not rightfully parties to, or authorized to act on behalf of, Plaintiff with respect to the Plaintiff-Merchant Agreements, Plaintiff's rights under the BCX-Merchant Agreements, or any other contracts.

3. Defendants intentionally and without justification or excuse unreasonably and actually interfered with these Agreements and contracts.

4. As a direct and proximate result of Defendants' interferences, Plaintiff has been damaged.

5. Plaintiff has suffered, and will continue to suffer, irreparable harm as a result of Defendants' actions.

6. Defendants are liable for Plaintiff's damages.



**COUNT ELEVEN –BREACH OF EMPLOYMENT CONTRACT  
(as against Defendant Eduardo Park)**

1. Plaintiff repeats the allegations set forth in the preceding paragraphs as if fully set forth herein verbatim.
2. Eduardo entered into a valid Employment Agreement with Plaintiff not to collect, remove or use Plaintiff's data absent Plaintiff's written permission.
3. Plaintiff at all times complied with the terms of its contract with Eduardo.
4. The parties' contract was reasonable as to time and scope of activity.
5. The parties' contract was necessary to protect the legitimate interests of Plaintiff.
6. The parties' contract was not unduly burdensome to Eduardo.
7. The parties' contract was not injurious to the public interest.
8. Eduardo, BCX, Ethan, and Defendants to be discovered knew of the covenant and inured benefit from its breach.
9. As a result of Eduardo's misconduct, Plaintiff is entitled to specific performance.
10. Eduardo, BCX, Ethan, and Defendants to be discovered are liable in damages to Plaintiff for the proximate consequences of the breach of said covenant.

**COUNT TWELVE – BREACH OF THE IMPLIED COVENANT OF  
GOOD FAITH AND FAIR DEALING  
(as against Defendant Eduardo Park)**

1. Plaintiff repeats the allegations set forth in the preceding paragraphs as if fully set forth herein verbatim.
2. Eduardo was bound by a duty of good faith and fair dealing in both the performance and enforcement of his Employment Agreement with Plaintiff.
3. Plaintiff relied upon Eduardo's representations that he would, in good faith, abide by the terms of the parties' Employment Agreement.

4. Plaintiff at all times fully complied with all acts required of it under the implied covenant of good faith and fair dealing in its contractual relations with Eduardo.

5. Eduardo's conduct was unfaithful to the agreed common purpose and inconsistent with the justified expectations of Plaintiff. Eduardo breached his obligation of good faith and fair dealing by engaging in the activities more fully described hereinabove.

6. Eduardo's conduct will have the effect of destroying or injuring Plaintiff's right to receive the benefits of its Employment Agreement with Eduardo.

7. Eduardo acted with subterfuge, evasion and bad faith to deny the benefit of the bargain originally intended by these parties.

8. As a direct and proximate result of Eduardo's breach of his obligation of good faith and fair dealing, Plaintiff has suffered harm in the form of loss of business and/or profits, prospective economic advantage, goodwill in its relationships with customers and potential customers, and through disclosure, use and/or destruction of its confidential, trade secret and/or proprietary information.

9. Plaintiff is therefore entitled to specific performance and damages.

**COUNT THIRTEEN – UNJUST ENRICHMENT  
(as against all Defendants)**

1. Plaintiff repeats the allegations set forth in the preceding paragraphs as if fully set forth herein verbatim.

2. Plaintiff accumulated its intellectual property, including confidential trade secret information over a period of some two decades.

3. Plaintiff's information, data and know-how regarding POS equipment, processing and service, suppliers, customers, prices and the like are unique and valuable.

4. At present, such information is directly benefitting Defendants, without compensation, payment, remuneration, royalties or services of any kind or nature to Plaintiff.

5. As such, BCX, Eduardo, Ethan, and the Defendants to be discovered have been unjustly enriched. This unjust enrichment has come at the expense of Plaintiff.

6. It would be unjust for said Defendants to retain the confidential trade secret information and data copied by Defendants for their use.

7. It would be unjust for said Defendants to retain any revenues derived from their misappropriation, use and destruction of Plaintiff's data, and confidential trade secret information taken by Defendants for their use.

8. As a direct and proximate result of Defendants' unjust enrichment, Plaintiff has been damaged.

**COUNT FOURTEEN – BREACH OF THE DUTY OF LOYALTY  
(as against Defendant Eduardo Park)**

1. Plaintiff repeats the allegations set forth in the preceding paragraphs as if fully set forth herein verbatim.

2. Eduardo was, at all times relevant hereto, an employee of Plaintiff.

3. Eduardo violated his duty of loyalty to Plaintiff by conduct including, without limitation:

- a. Taking a position with BCX before the contractual exclusion expired;
- b. Taking a position with BCX to compete directly with Plaintiff;
- c. Aiding Plaintiff's direct competitor and/or those with interests adverse to Plaintiff's interest;
- d. Participating in a plan to vitiate, destroy or otherwise injure Plaintiff's business and data;



- e. Depriving Plaintiff of economic opportunities; and
- f. Taking affirmative steps to injure Plaintiff's business.

4. Eduardo is liable to Plaintiff for equitable relief and damages proximately caused by his breach of the duty of loyalty to Plaintiff.

**COUNT FIFTEEN – AIDING AND ABETTING  
(as against all Defendants)**

1. Plaintiff repeats the allegations set forth in the preceding paragraphs as if fully set forth herein verbatim.

2. BCX, Ethan, Eduardo and Defendants to be discovered knew that Eduardo's conduct constituted a breach of duty.

3. Defendants gave substantial assistance or encouragement to Eduardo to conduct himself thus.

4. By receiving and using Plaintiff's confidential and trade secret information, BCX, Ethan, and Defendants to be discovered, acted in concert with Eduardo or pursuant to a common design with him.

5. BCX, Ethan, and Defendants to be discovered, knowingly gave substantial assistance to Eduardo in accomplishing a tortious result and their own conduct, separately considered, constitutes a breach of duty to Plaintiff.

6. As a direct and proximate result of the aiding and abetting of Eduardo's tortious conduct by BCX, Ethan, and Defendants to be discovered, Plaintiff has been severely damaged.

**PRAYER FOR RELIEF**

**WHEREFORE**, the Plaintiff INNOAS, INC. demands judgment, jointly, severally, and/or individually, against Defendants VISTA CAPITAL, LLC d/b/a BANCARDXPRESS; ETHAN PARK; EDUARDO PARK; XYZ CORPORATIONS 1–10 (fictitious); and John/Jane Does 1–10

(fictitious), for preliminary and final mandatory injunction compelling all Defendants to surrender his/its/their computers, digital equipment, data and logs to Plaintiff, and also an order or prohibitory injunction, prohibiting Defendants from accessing, copying, deleting, possessing, transferring or in any way using Plaintiff's data, confidential and trade secret information; for damages, including without limitation direct, compensatory and exemplary damages, further including treble damages where so provided; and for reasonable attorneys' fees and, costs, and for other such relief as the Court may deem to be necessary and proper, in the interest of justice.

**JURY DEMAND**

Plaintiff hereby demands a trial by a jury on all of the triable issues of this Complaint.

Dated: December 1, 2017

By: /s/ Joshua S. Lim  
Joshua S. Lim, Esq.  
KIM, CHO & LIM, LLC  
460 Bergen Blvd., Suite 305  
Palisades Park, New Jersey 07650  
Tel: 201-585-7400  
*Attorneys for Plaintiff*